ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIL Verification

Slide 6 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Types of Failures - Recap

- Sub Systems can fail because of:
  - Random hardware failures
  - Common cause hardware failures
  - Systematic failures
- Any of these failures drives the SIF into a specific state:
  - Safe failures λ_s = Safe undetected failure rate λ_{su} + Safe detected failure rate λ_{sd}
  - Dangerous failures λ_d = Dangerous undetected failure rate λ_{du} + Dangerous detected failure rate λ_{dd}

Slide 6 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic Failures - Recap

- **Definition: A hidden fault in design or implementation such:**
  - Software design
  - Specifications
  - Operating manuals
  - Maintenance or test Procedures, etc
- **IEC 61508 approach:**
  - Measures to avoid systematic failures ((tables in 61508-2/3 Annex A/B))
  - Probabilistic calculations for Software can be done (61508-7 Annex D)

Slide 6 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Hardware Verification Approaches:

- **IEC 61511-2 approach:**
  - Follow Methodology in IEC 61508-2 & 3 Annex B for hardware systematics
  - Hardware Verification – IEC 61508 or ISA simplified approach allowed
- **IEC 61508-6 approach:**
  - Techniques and Measures to control systematic hardware failures (tables in 61508-2/3 Annex A/B)
  - Hardware Verification (PFD or PFH Calculation)
- **ISA-TR84.00.02-2002 approach:**
  - Detailed Technical Report on 5 Parts - Simplified Equations, FTA, Markov Analysis

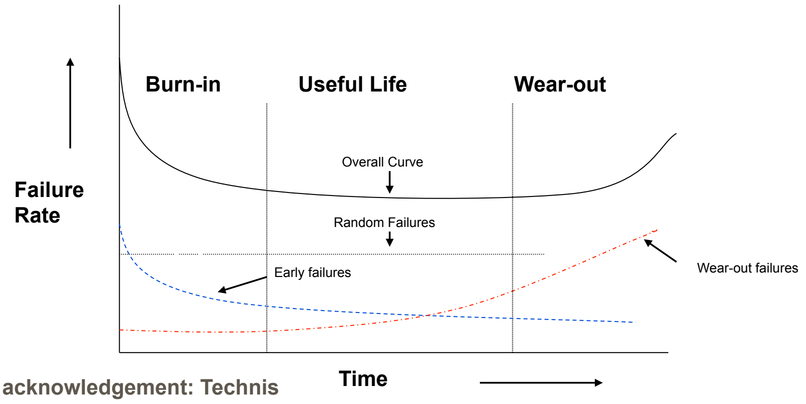
Slide 6 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Random Hardware Failures - Introduction

The Bathtub Curve & Assumed Constant Failure rate



Slide acknowledgement: Technis

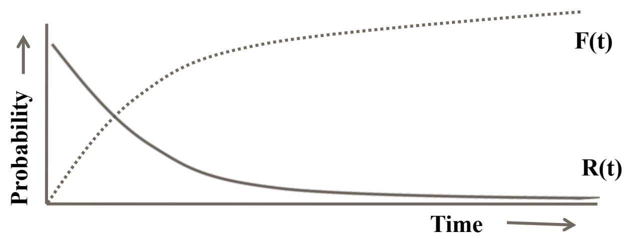
Slide 6 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Simplified Exponential Distribution - Background

- IEC 61508 / 61511 equations assume a Constant failure rate = λ
- Therefore the exponential distribution can be simplified to -
- Reliability rate – $R(t) = e^{-\lambda t}$
- Unreliability rate – $F(t) = 1 - R(t)$
- Unreliability rate – $F(t) = 1 - e^{-\lambda t}$ (Cumulative Probability of failure)
- If λt is small (<0.1), then $1 - e^{-\lambda t}$ approximates to λt



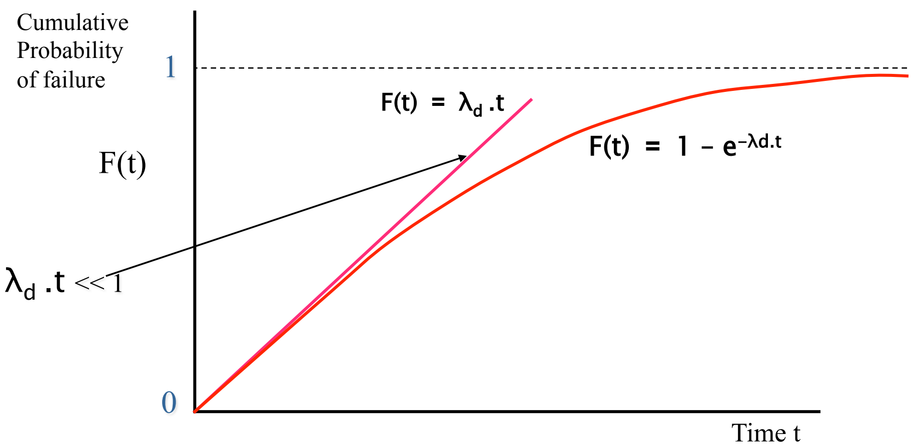
For a detailed discussion of the simplification refer to Reliability, Maintainability & Risk" Smith – ISBN 978-0-7506-6694-7

Slide 6 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Cumulative Probability of Failure – Linear Assumption



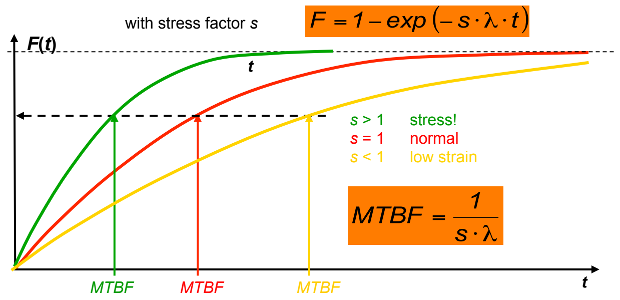
Slide 6 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The effects of Stress on component Failure - Background

The probability of failure changes under different stress conditions:

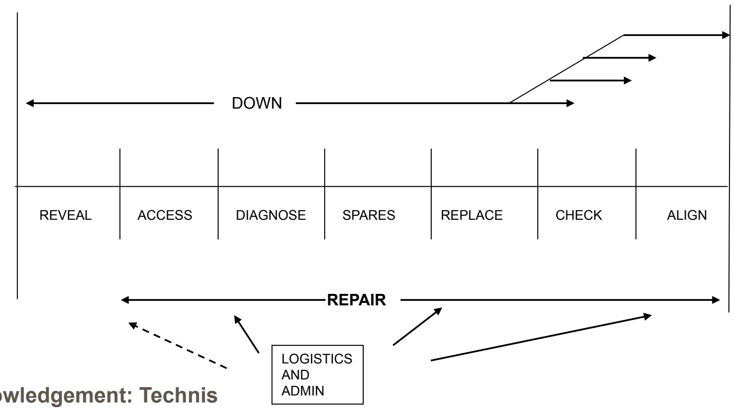


Slide 6 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Considering the Mean Time To Repair (MTTR)



Slide acknowledgement: Technis

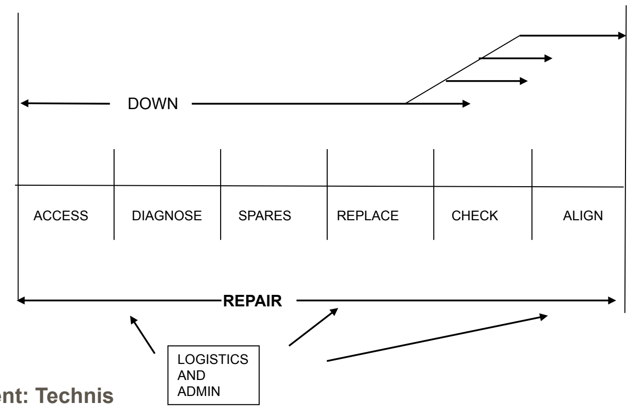
Slide 6 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Considering the Mean Repair Time (MRT)

MRT does not include the time to detect the failure



Slide acknowledgement: Technis

Slide 6 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Considering the MEAN DOWN TIME (MDT)

Of any unit:

MRT + (Proof Test Interval)/2

1

Of a System with two Redundant Units:

MRT + (Proof Test Interval)/3

1 **2**

Slide acknowledgement: Technis

Slide 6 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Definitions - Unavailability and Availability - Background

For a 1oo1 System - 10 yrs MTBF; annual proof test interval (PTI) means:

Assume 1/MTBF = λ (when << 1) = 1/10 = 0.1

MDT = MRT + PTI/ 2 = 0.5 (Assuming MRT is small e.g. 4 hours)

Thus Unavailability = 0.5 yr x 0.1 pa = 5% = PFD = 0.05

Unavailability ≡ λ MDT (Approximation when λ is small)

UNAVAILABILITY is similar to PFDavg

NB: actually λ MDT / (1 + λ MDT) (For when λ is large)

NB: Availability = 1 – Unavailability

NB: Availability = MTTF / (MTTF + MTTR)

NB: MTBF = MTTF + MTTR

Slide 6 - 12

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Understanding Types of Failure Rate Data

- Generic Data
- Industry specific data
- Site specific data

The type of data used affects the accuracy of the prediction

Slide 6 - 13

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Examples of Failure Data Sources

- US MIL Handbook 217
- UK BT HRD
- Lees “Loss Prevention in the Process Industries”
- AIChemE – Process Equipment Reliability Data Book
- OREDA, PDS, SINTEF Data Book (Offshore)
- Exida Safety Data Handbook
- Manufacturers FMEDA Reports
- UK MoD Def Stan 00-41
- UKAEA (SRD)
- Faradip
- Various Consultants data banks RMC, DNV, DJS
- SN 29500

Slide 6 - 14

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example of using Failure Rate Data - Faradip

	PER MILLION HOURS		
Gas pellister 1010(fail .003)	5.00	10	30
Detector smoke ionization	1.00	6.00	40
Detector ultraviolet	5.00	8.00	20
Detector infra red (fail .003)	2.00	7.00	50
Detector rate of rise	1.00	4.00	12
Detector temperature	0.10	2.00	.
Detector flame failure	1.00	10	200
Detector gas IR (fail .003)	1.50	5.00	80

Failure modes (proportion)		
Rate of rise	Spurious 0.6	Fail 0.4
Gas pellister	Spurious 0.3	Fail 0.7
Infra red	Spurious 0.5	Fail 0.5
Smoke (ionize) & UV	Spurious 0.6	Fail 0.4

Slide acknowledgement: Technis

Slide 6 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Estimating Confidence Levels for Failure Data

"Reliability, Maintainability & Risk" Smith – ISBN 978-0-7506-6694-7

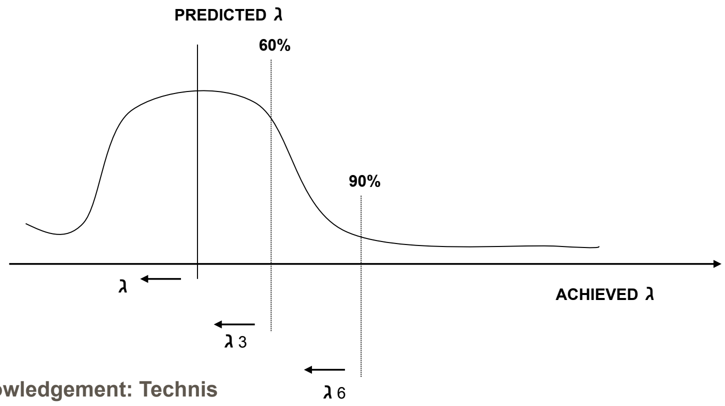
- Smith proposes rules of thumb for estimating the confidence level for:
  - Generic Data
  - Industry specific data
  - Site specific data

Slide 6 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Increasing Confidence Levels when Using Generic Data



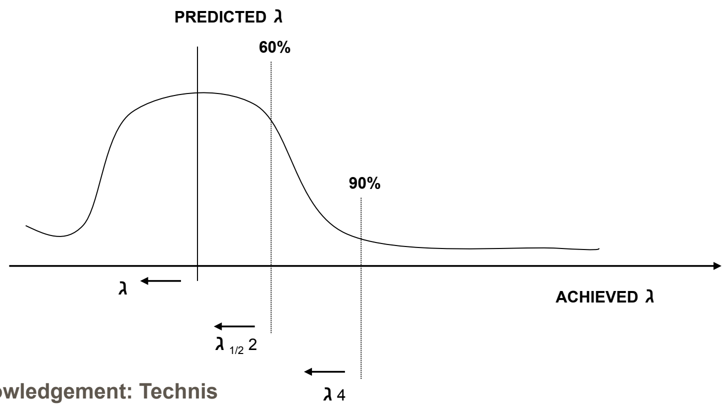
Slide acknowledgement: Technis

Slide 6 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Increasing Confidence Levels when Using Industry Data



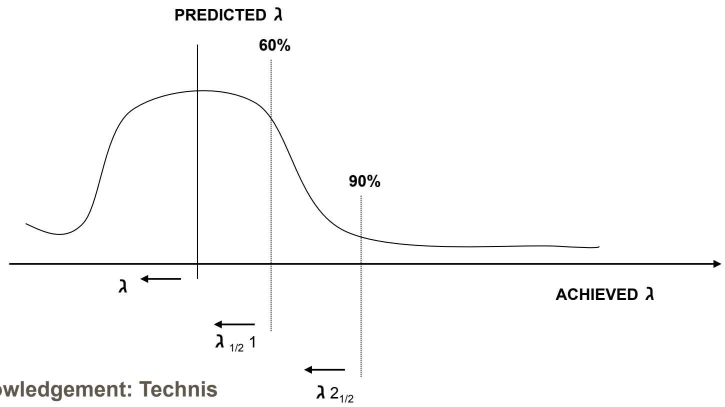
Slide acknowledgement: Technis

Slide 6 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Increasing Confidence Levels when Using Site/Company Data



Slide acknowledgement: Technis

Slide 6 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Failure Mode, Effect Analysis (FMEA)

Slide 6 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Failure Modes and Effect Analysis (FMEA)

- Purpose – to study the results or effects of item failure on system operation and to classify each potential failure according to its severity
  - First formal applications in1960 in the aerospace industry
  - First of all it is a design technique
  - But is also a verification technique
  - It can be used for products, systems and processes
  - Is a single failure mode analysis technique
  - Does not consider multiple failures at the same time
  - Common cause or systematic failures are not addressed
  - Is a bottom-up technique

Slide 6 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

FMEA can be adjusted to the problem or needs at hand

- FMEA – Failure modes and effects analysis
  - Basic technique (BS EN 60812)
  - DOD MIL-STD-1629A
- FMECA – Failure mode, effect, and critically analysis
- Functional FMEA
- Maintenance FMEA
- Process FMEA
- Software FMEA
- FMEDA – Failure modes, effects and diagnostic analysis

Slide 6 - 22

Functional Safety Engineering

FMEA Process

- The following steps are important
  - Define the system and scope of the analysis
  - List all sub systems and components
  - Identify failure modes
    - Determine rates of occurrence
    - Determine Locatability
  - Identify effects of failure
    - Determine severity
    - Determine detectability – Locatability – Fault Coverage (FD/FL)
    - Criticality Analysis

Slide 6 - 23

Functional Safety Engineering

Example Failure Mode & Effect Aanalysis

Severity Classification

1	Fault leading to an Unsafe Failure which is not detected by the system diagnostics
2	Fault leading to an Unsafe Failure which is detected by the system diagnostics
3	Fault leading to a Safe Failure which is not detected by the system diagnostics
4	Fault leading to a Safe Failure which is detected by the system diagnostics

Identification	Function	Failure Modes	Operational Mode	Failure Effects		Detection Method	Compensating Provisions	Severity Class	Remarks
				Local	End				
Temperature Controlled Reference Coils	Provide reference against which measured values can be compared	Fibre Break	Normal	No Profile	Incorrect Trace	Normal operation reports break and location	Redundant DTS 800 M4 Unit	4	Requires replacement of Optics Module. One instance in fault reports.
Fibre Switch	Allows single laser to connect to multiple fibres	Switch dirty	Normal	Source attenuated	Degraded trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	Unit can be cleaned
Receiver	Detects Back scattered light	Surface Degradation	Normal	Reduction in output	Degraded Trace	QA Zone allocated for Signal Level Below threshold	Redundant DTS 800 M4 Unit	4	Long term gradual failure
Laser (Inc AOD)	Generate Light source for transmission through fibre sensors	Reduction in Power	Normal	Source attenuated	Degraded Trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	Most recorded fault
AOD Driver	Provides pulsing function of laser	Incorrect Pulse - Believable	Normal	Close to correct emission profile	Potential error in temperature value	QA Zone allocated to monitor Standard Deviation. Periodic Function Test.	Redundant DTS 800 M4 Unit	2	Include trace analysis for this fault in periodic site Function Test.
Breakout PCB	Provides power distribution for Optics Module	Incorrect Voltage to other circuits	Normal	Module supply out of spec	Degraded Trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	Most sensitive module is processor which will shut down switching outputs to safe state.
Main Amp	Amplifies Optics Module output for processing	Incorrect Gain	Normal	Incorrect signal to Averager	Incorrect Trace	QA Zone allocated for Signal Level Below threshold	Redundant DTS 800 M4 Unit	4	Does not affect reported values, but signal could be biased. Detectable during periodic FunctionTest. Reference signal offset as per measured signal.
Temperature Control PCB Assembly	Controls temperature of laser, receiver, reference coil and AOD.	Temperature sensor fault	Normal	Incorrect control level	On Ref Coil, trace will be offset	Functional Test by applying shock low temp to field sensor.	Redundant DTS 800 M4 Unit	1	Trip threshold is against an absolute level. This fault could mean that the absolute threshold is not reached therefore no trip. However, there are no reports of this failure mode in fault records.
Optics Interface PCB Assembly	Gain and offset to main amp plus HV supplies to APD's	Incorrect gain & offset to Main Amp.	Normal	Incorrect signal to Averager	Incorrect Trace	QA Zone allocated for Signal Level Below threshold	Redundant DTS 800 M4 Unit	4	Does not affect reported values, but signal could be biased. Detectable during periodic FunctionTest. Reference signal offset as per measured signal.
Averager PCB Assembly	Accumulates data and generates average	A/D Converter Fail	Normal	No Output	No Trace	QA Zone allocated for Signal / Noise ratio above threshold	Redundant DTS 800 M4 Unit	4	
Power Supply	Provides power & regulation to system modules	Output Too Low	Normal	Some Modules Failing	Degraded or No Trace	Alarm handoff from UPS to serial interface. QA Zone allocated for Signal / Noise ratio above threshold.	UPS with battery pack. Redundant DTS 800 M4 Unit	4	
Memory PCB Assembly	Stores OS, Application and data.	Data Corrupted	Normal	Wrong results	Inconsistent Data, incorrect operation of relays	QA Zones set up for inconsistency checking	Redundant Unit	4	
Processor PCB Assembly	Perform mathematical analysis on returned signals	Incorrect Calculation	Normal	Incorrect result	Inconsistency in Trace	QA Zone detects abnormal trace.	Redundant DTS 800 M4 Unit.	2	Project uses redundant pair. One processor in error would lead to discrepancy between units detected by safety logic solver, but possibly only when trip condition occurs.
Output Module	Provide powered outputs to interposing relays to external logic solver	Contacts stick closed	Normal	Fail to open on demand from processor	Failure to transfer status to safety system	Voting in comparison with redundant 800 DTS system in external safety logic solver. Comparison with fault relay status.	Redundant DTS 800 M4 Unit. Selection of relays with low fail rates	1	Original on-board relays now removed and replaced by external high quiality relays incorporating Hermetic seal and gas filled can.

Slide 6 - 24

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault Tree Analysis (FTA)

Slide 6 - 25

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

WHAT IS FAULT TREE ANALYSIS

- An analysis method to identify causes for an assumed failure (top event)
- Deductive method – focuses on top event
- Logical structure
- Considers Equipment failures & Human errors
- Identify possible causes for a system failure
- Predict:
  - Reliability
  - Availability
  - Failure frequency
- Identify system improvements
- Predict effects of changes in design and operation

Slide 6 - 26

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault Tree Symbols

TOP — Tank Over Spill

INTERMEDIATE — No High Level Alarm

BASIC — Level Switch Failed

LS

- Basic event data are normally failure frequencies.
- Conversion to probability depends on whether failure is revealed or unrevealed.

Slide 6 - 27

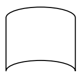
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Fault Tree Symbols- 2

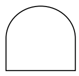
LOGIC GATES:

OR gate



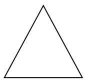
Output occurs if any of the input events happen

AND gate



Output occurs only when all the input events happen

TRANSFER gate



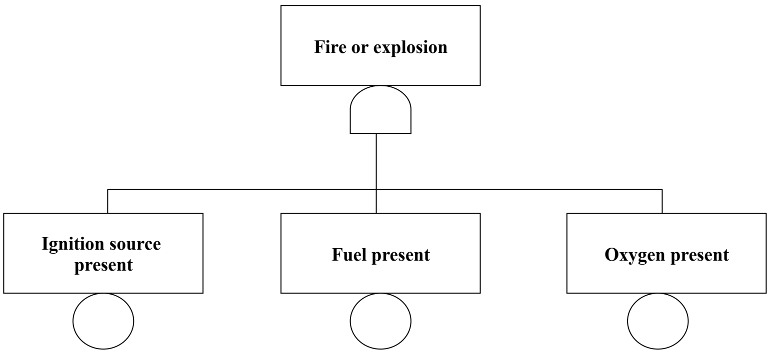
Indicates that part of this fault tree is developed elsewhere

Slide 6 - 28

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

AND gate example



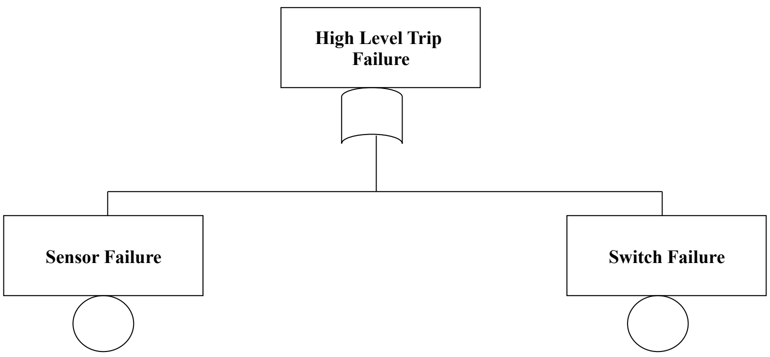
Output event occurs only when all the input events happen

Slide 6 - 29

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

OR gate example



Output event occurs in any of the input events happen

Slide 6 - 30

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process

STEP 1 -	System Definition
STEP 2 -	Understanding the system
STEP 3 -	Defining the top event
STEP 4 -	Constructing the fault tree
STEP 5 -	Qualitative Analysis
STEP 6 -	Gather failure rate data
STEP 7 -	Quantitative Analysis

Slide 6 - 31

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process- 2

Step 1 - System Definitions

- Mark-up system drawing and check off items
- Initial equipment configuration
  - Which valves open/closed / Which pumps on/off?

Step 2 - Understanding the System

- Un-allowed events (considered not possible)
- Existing events (considered certain)
- Other assumptions

Step 3 - Top Event Identification

- Requires precise definition - Use HAZOP, FMEA, experience etc
- Vague or poorly defined top events often lead to a poor analysis
- Example: - 'Compressor Fire' is too general use 'Fire in the oxygen compressor enclosure during normal operation' is good

Slide 6 - 32

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 3

Step 4 - Fault Tree Construction

- Begin at top event
- Determine the intermediate faults/causes that result in the top event
- If the basic causes can be determined immediately from the top event then the problem is too simple for FTA
- Identify the logic gate that defines the relationship of those causes to the top event.
- **HOW FAR TO GO?**
  - A branch is of no further interest
  - A branch is known to have very low probability
  - You have reached the stage of individual component failures for which no data is available

Slide 6 - 33

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 4

STEP 5 – Fault Tree Reduction (Qualitative Analysis)

- A cut set is any combination of basic events which will cause the top event.
- Cut sets are calculated by Boolean algebra (for complex fault trees many thousands of cut sets may be produced – therefore only simple trees are produced and quantified by hand?.
- Cut sets are used to quantify fault trees.

- 1^{st} Order - 1 Event causes top entry
- 2^{nd} Order - 2 Events needed top entry
- 3^{rd} Order - 3 Events needed top entry

Slide 6 - 34

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Boolean Algebra

1. AND (A and B) = $A.B$
2. OR (A or B) = $A+B$
3. NOT (A) = $\bar{A}$
4. XOR (A and B) = $A.\bar{B} + B.\bar{A}$

1. $A+A = A$
2. $A + 1 = 1$
3. $A + 0 = A$
4. $A.A = A$
5. $A.1 = A$
6. $A.0 = 0$
7. $A+A.B = A$
8. $A + \bar{A} = 1$
9. $A.\bar{A} = 0$
10. $\overline{A.B} = \bar{A}+\bar{B}$
11. $\overline{A+B} = \bar{A}.\bar{B}$

Slide 6 - 35

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 5

Step 6 – Gathering Failure Data

- Need data on basic event frequencies/probabilities.
- Site historical data is preferred when not available take from reliability database such as Faradip etc
- Engineering judgment needed when data is sparse

Step 7 – Fault Tree Quantification

- Calculation of top event frequency or probability
- How often? = Frequency
- Chance of failure on demand = Probability

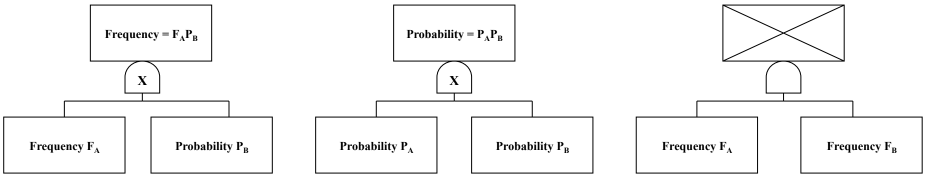
Slide 6 - 36

ProSalus SAFETY CONSULTANTS

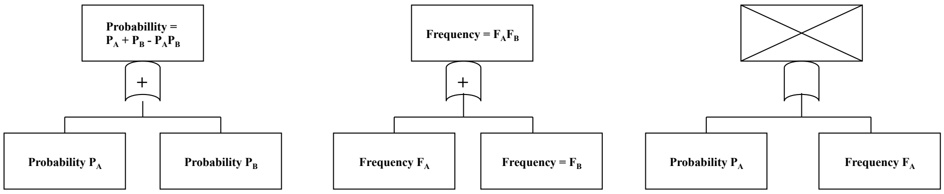
Functional Safety Engineering

Gate By Gate Calculation

AND Gate



OR Gate



Slide 6 - 37

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Rules For Quantification

1 All branches must be independent

2 Decide if top event probability (P) or frequency (F) is required

3 Obtain failure data and convert to probability if required.

Revealed Failure: P = F x Repair Time
Unrevealed Failure: P = 0.5 x F x Test Interval

4 OR Gates (Add)
All inputs must be same type as output

5 AND Gates (Multiply)
P_a x P_b = P; F_a x P_b = F; F_a x F_b not permitted

Slide 6 - 38

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The FTA Process - 6

Common Mode/Dependent Failures

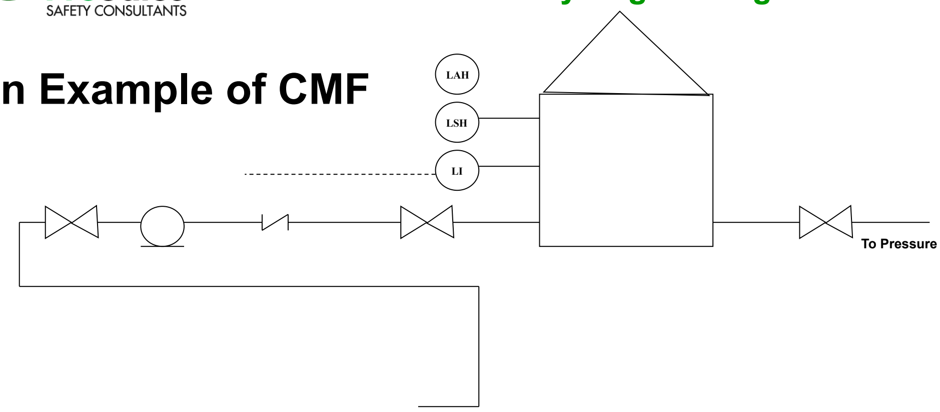
- Quantification assumes all events independent
- CMF causes a number of things to fail simultaneously
- CMF can cause serious errors in results if not included in fault tree
    - Defeats redundancy and/or diversity
    - Can involve both initiating event and mitigating systems

Slide 6 - 39

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

An Example of CMF



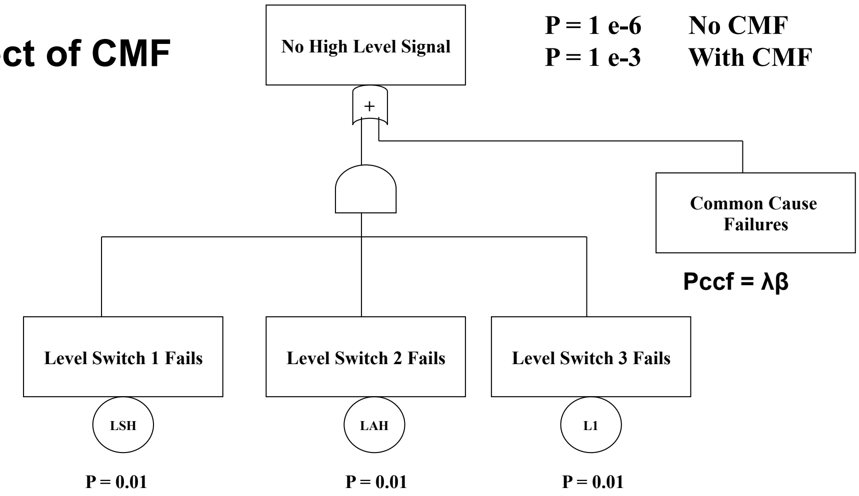
- **Danger of overfilling tank, with potential to overpressure tank. Protect with 3 independent high-level shutdown systems?**

Slide 6 - 40

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Effect of CMF



Slide 6 - 41

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

STRENGTHS OF FTA

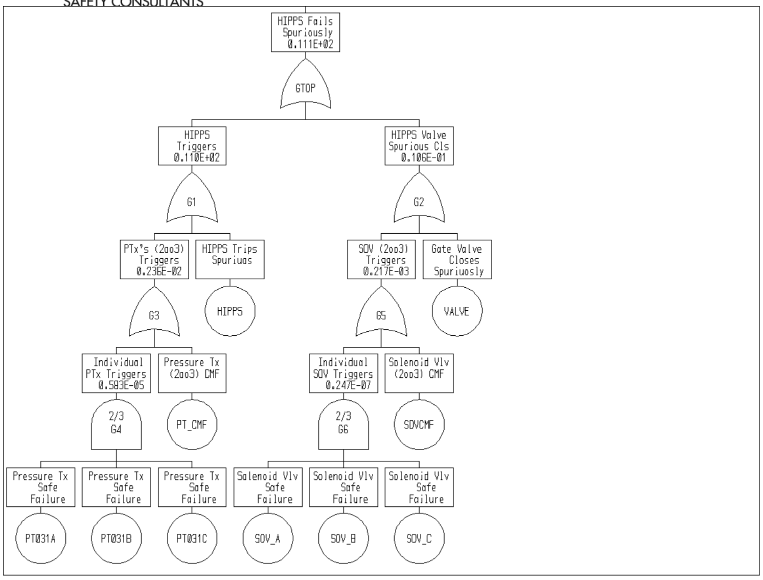
- Widely used
- Theory well developed
- Many published texts and papers
- Large number of engineers trained in FTA
- Complimentary information available from:
  - Qualitative and
  - Quantitative analysis
- Visually easy to understand

Weakness of FTA

- Very time consuming
- Errors if paths missed
- Error prone if manual
- Substantial experience needed
- Poor treatment of time dependence

Slide 6 - 42

Functional Safety Engineering



FTA SIL Verification Example

Slide 6 - 43

Functional Safety Engineering

Architectures for
Low Demand mode of Operation

Based on ISA.TR84.00.02-2002

Slide 6 - 44

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ISA TR 84.00.02 (Part 1 & 2) Simple Formulas– Basic of terms

β	The fraction of undetected failures that have a common cause
λ_{DCCF}	$\beta\lambda_D$
λ_D	Dangerous failure rate
λ_{DD}	Detected dangerous failure rate
λ_{DU}	Undetected dangerous failure rate
MTTR	Mean time to repair
PFD_{AVG}	Average probability of failure on demand
T_i	Proof – test interval
λ_s	Safe failure rate
DC	Diagnostic Coverage DC = λ_{DD}/λ_D
T_{ia}	Auto Diagnostic Test Interval

Slide 6 - 45

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

ISA TR 84.00.02 (Part 1 & 2) Simple Formulas - Approximation

	1oo1	1oo2	1oo3	2oo2	2oo3
PFDavg	$\frac{1}{2}\lambda_d T_i$	$\frac{1}{3}\lambda_d^2 T_i^2$	$\frac{1}{4}\lambda_d^3 T_i^3$	$\lambda_d T_i$	$\lambda_d^2 T_i^2$
STR	λ_s	$2\lambda_s$	$3\lambda_s$	$2\lambda_s^2$MTTR	$6\lambda_s^2$MTTR

λ_d = Dangerous failure rate

λ_s = Revealed failure rate

T_i = Test interval

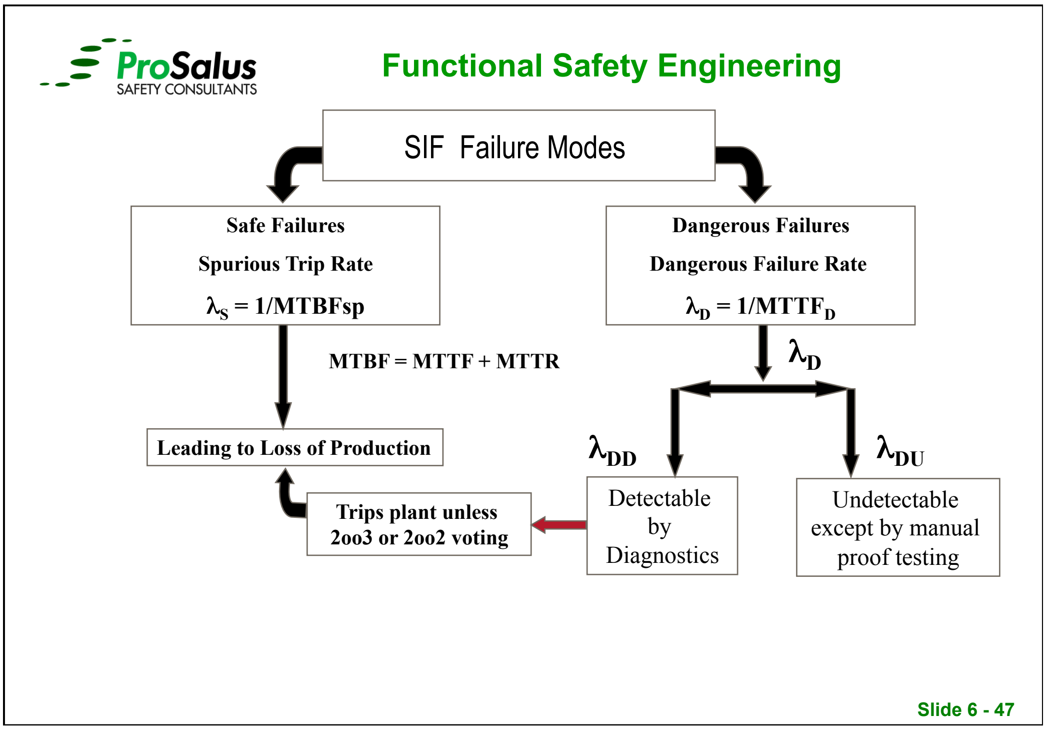
MTTR = Mean Time to repair

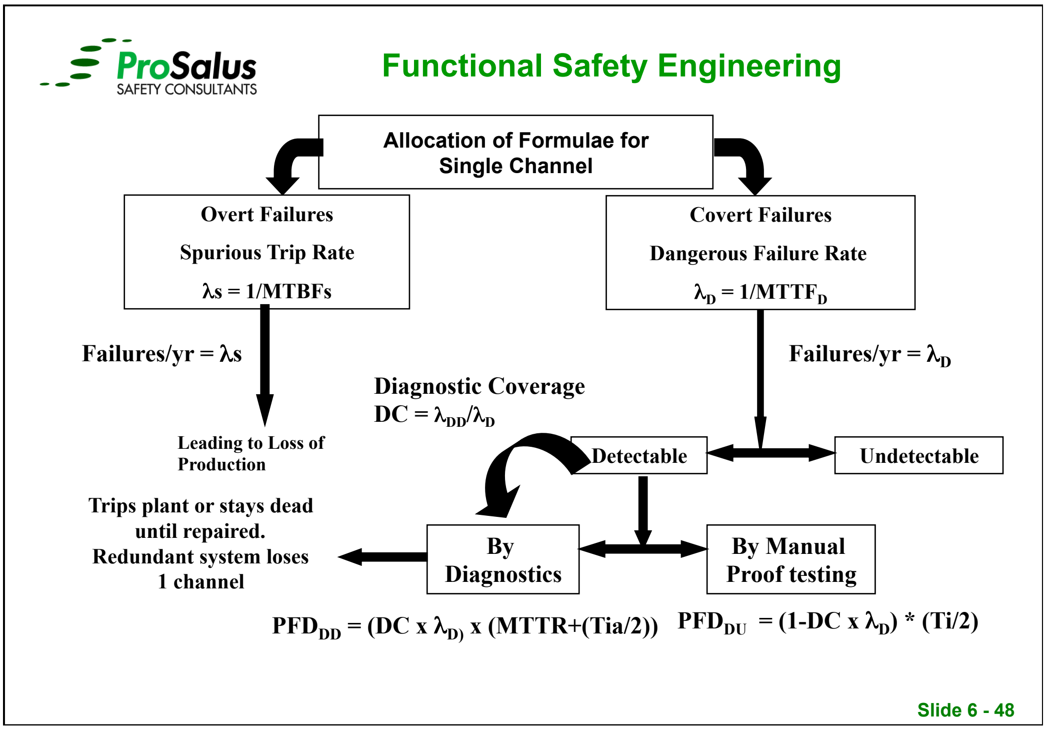
Table showing the most basic simple formula’s.

These formula’s do not take into account:

- Test coverage factor
- Maintenance interval
- Test duration
- Override during repair
- CCF (Beta Factor)
- Systematic failure rate

Slide 6 - 46


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
SIF Failure Modes
Safe Failures
Spurious Trip Rate
λ_S = 1/MTBFsp
Dangerous Failures
Dangerous Failure Rate
λ_D = 1/MTTF$_D$
MTBF = MTTF + MTTR
λ_D
Leading to Loss of Production
λ_{DD}
λ_{DU}
Trips plant unless 2oo3 or 2oo2 voting
Detectable by Diagnostics
Undetectable except by manual proof testing
Slide 6 - 47


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
Allocation of Formulae for Single Channel
Overt Failures
Spurious Trip Rate
λs = 1/MTBFs
Covert Failures
Dangerous Failure Rate
λ_D = 1/MTTF$_D$
Failures/yr = λs
Failures/yr = λ_D
Diagnostic Coverage
DC = λ_{DD}/λ_D
Leading to Loss of Production
Detectable
Undetectable
Trips plant or stays dead until repaired.
Redundant system loses 1 channel
By Diagnostics
By Manual Proof testing
PFD$_{DD}$ = (DC x $\lambda_{D)}$ x (MTTR+(Tia/2))
PFD$_{DU}$ = (1-DC x λ_D) * (Ti/2)
Slide 6 - 48

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

PFD_{avg} Calculations According to ISA.TR84.00.02-2002

The PFD_{avg} is determined by calculating the PFD for all of the components in each SIF loop and combining these individual values to obtain the overall SIF loop PFD_{AVG} value. This is expressed by the following:

$$PFD_{SIF} = \Sigma PFD_s + \Sigma PFD_{Ls} + \Sigma PFD_{FE}$$

Where,

PFD_{FE} is the final element PFD_{avg} for a specific SIF,

PFD_S is the sensor PFD_{avg} for a specific SIF,

PFD_{LS} is the logic solver PFD_{avg},

PFD_{SIF} is the PFD_{avg} for the specific SIF in the SIS.

Slide 6 - 49

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Determining the PFD_{avg} (ISA.TR84.00.02-2002)

The procedure for determining the PFD_{avg} is as follows:

1.Identify each sensor that detects the process condition that could lead to the event the SIF is protecting against

Only those sensors that prevent or mitigate the designated event are included in PFD calculations.

2.List the $MTTF^{DU}$ for each sensor.

3.Calculate the PFD for each sensor configuration using the $MTTF^{DU}$ and the appropriate equation with consideration for redundancy.

Slide 6 - 50

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

System Equations (ISA.TR84.00.02-2002)

The following equations cover the typical configurations used in SIF configurations. To see the derivation of the equations listed, refer to ISA–TR84.0.02–Part 5.

Converting MTTF to failure rate, λ:

$$\lambda^{DU} = 1 \setminus MTTF^{DU}$$

Equations for typical configurations:

$$\textbf{1oo1}\ PFD_{avg} = [\lambda^{DU} \times TI/2] + [\lambda^{D}_{F} \times TI/2]$$

Where λ^{DU} is the undetected dangerous failure rate
λ^{D}_{F} is the dangerous systematic failure rate, and
TI is the proof test interval

Slide 6 - 51

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Systematic Failures (ISA.TR84.00.02-2002)

ISA equations model the systematic failure λ^{D}_{F} as an error that occurred during the specification, design, implementation, commissioning, or maintenance that resulted in the SIF component being susceptible to a random failure.

Systematic failures are rarely modeled for SIF Verification calculations due to the difficultly in assessing the failure modes and effects and the lack of failure rate data for various types of systematic failure.

However, these failures are extremely important and can result in a significant impact to the SIF performance, this is addressed through lifecycle process that incorporates design and installation concepts, validation and testing criteria, and management of change and are intended to to be a defense systematic failures..

Slide 6 - 52

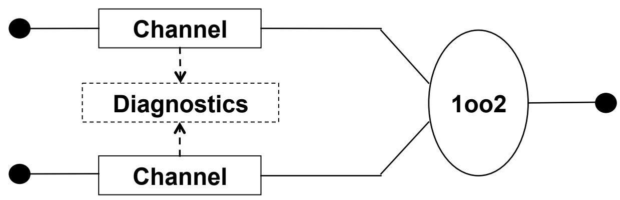
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 (ISA.TR84.00.02-2002)

1oo2 - System

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.



1oo2 physical block diagram

Slide 6 - 53

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 (ISA.TR84.00.02-2002)

PFD_{avg} = [((1-β) x λ^{DU})^{2}x TI^2/3] + [(1-β) x λ^{DU} x λ^{DD} x MTTR x TI] + [β x λ^{DU} x TI/2] + [λ^{D}_{F} x TI/2]

For simplification, 1 – β is generally assumed to be one, which yields conservative results. Consequently, the equation reduces to

PFD_{avg} = [(λ^{DU})^2 x TI^2/3] + [λ^{DU} x λ^{DD} x MTTR x TI] + [β x λ^{DU} x TI/2] + [λ^{D}_{F} x TI/2]

Where MTTR is the mean time to repair
λ^{DD} is dangerous detected failure rate, and
β is fraction of failures that impact more than one channel of a redundant system (CCF).

The second term represents multiple failures during repair. This factor is typically negligible for short repair times (typically less than 8 hours). The third term is the common cause term. The fourth term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate λ_s = Safe failure rate channel 1 (λ_{s1})
+ Safe failure rate channel 2 (λ_{s2})

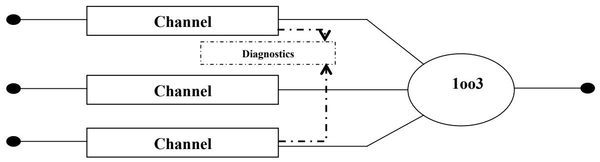
Slide 6 - 54

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

1oo3 (ISA.TR84.00.02-2002)

1oo3 – System
This architecture consists of three channels connected in parallel, such that either channel can process the safety function. Thus there would have to be dangerous failure in all three channels before a safety function failed on demand.



1oo3 physical block diagram

$$PFD_{avg} = [(\lambda^{DU})^3 \text{ x } TI^3/4] + [(\lambda^{DU})^2 \text{ x } \lambda^{DD} \text{ x } MTTR \text{ x } TI^2] + [\beta \text{ x } (\lambda^{DU} \text{ x } TI/2)] + [\lambda^{D}_{F} \text{ x } TI/2]$$

The second term accounts for multiple failures during repair. This factor is typically negligible for short repair times. The third term is the common cause term and the fourth term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate λ_s = $3\lambda_s$

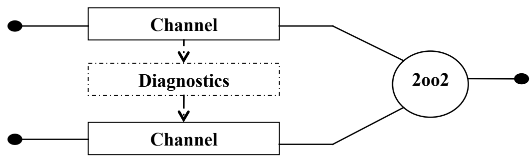
Slide 6 - 55

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering

2oo2 (ISA.TR84.00.02-2002)

2oo2 – System
This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.



2oo2 physical block diagram

$$PFD_{avg} = [\lambda^{DU} \text{ x } TI] + [\beta \text{ x } \lambda^{DU} \text{ x } TI] + [\lambda^{D}_{F} \text{ x } TI/2]$$

The second term is the common cause term and the term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate λ_s = $2\lambda_s^2 MTTR$

Slide 6 - 56

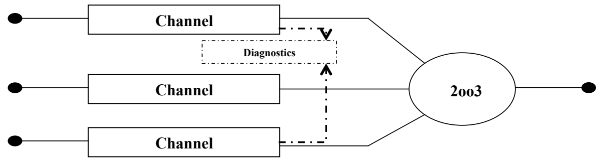
ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo3 (ISA.TR84.00.02-2002)

2oo3 – System

3 channels in parallel with majority voting such that the output state does not change if only 1 channel changes.



2oo3 physical block diagram

$PFD_{avg} = [(\lambda^{DU})^2 \times (TI)^2] + [3\lambda^{DU} \times \lambda^{DD} \times MTTR \times TI] + [\beta \times \lambda^{DU} \times TI/2] + [\lambda^{D}_{F} \times TI/2]$

The second term in the equation represents multiple failures during repair. This factor is typically negligible for short repair times. The third term is the common cause term. The fourth term is the systematic error term.

Spurious Trip Rate (STR) = Safe failure Rate $\lambda_s = 6\lambda_s^2 MTTR$

Slide 6 - 57

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The simplified equations **in** ISA.TR84.00.02-2002 without the terms for multiple failures during repair, common cause and systematic errors reduce to the following for general use

1oo1

$PFD_{avg} = \lambda^{DU} \times TI/2$

2oo2

$PFD_{avg} = \lambda^{DU} \times TI$

1oo2

$PFD_{avg} = [(\lambda^{DU})^2 \times TI^2]/3$

2oo3

$PFD_{avg} = (\lambda^{DU})^2 \times TI^2$

1oo3

$PFD_{avg} = [(\lambda^{DU})^3 \times TI^3]/4$

2oo4

$PFD_{avg} = (\lambda^{DU})^3 \times (TI)^3$

Slide 6 - 58

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Implementation

- Calculating the PFD of the function
  - The PFD of each subsystem/element is calculated for (1oo1, 1oo2 etc.) for the:
    - Initiator
    - Logic solver
    - Final element
  - The total PFD for the combination is then calculated

Slide 6 - 59

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Impact of Proof Testing

The Probability of Failure for 1oo1 element = $\frac{1}{2}\lambda_d T_i$

Therefore if the Proof test interval is increased then the PFDavg will also increases proportionally, likewise if the proof test is decreased the PFDavg will also decreases proportionally

Slide 6 - 60

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Impact of Maintenance

The simplified formula for PFDavg = $\frac{1}{2}\lambda_d T_i$

•Assumes that the element is in the 'as new condition'

•Testing does not cover every aspect (coverage factor < 1)

- E.g. we do not know the internal condition of a valve

•Only periodic 'bench type' maintenance can bring elements back to an 'as new condition'

•The PFDavg will increase without routine maintenance

Slide 6 - 61

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The Impact of Imperfect Proof Test and Maintenance

- At the Maintenance Interval the element is maintained and returned to the as new condition:
  - For 1oo1 System:

$$PFD_c = (\tfrac{1}{2}\lambda_d T_i C + \tfrac{1}{2}\lambda_d T_m (1 - C))$$

Where:
λd = Total unrevealed or dangerous failure rate (per/year)
Ti = Total interval (years)
C = The Proof test coverage factor
Tm = Maintenance interval; interval at which the device is maintained to as new condition (years)

Slide 6 - 62

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Calculation

For a simplified 1oo1 system:

$$PFDavg = ½\lambda_d T_i$$

Dangerous undetected failure rate λ is 10^{-6} h^{-1} (1 failure in 114 years)

Proof test Ti is annual (every 8760 hours),

So the

$$PFD_{avg} = 0.5 \cdot 10^{-6} \cdot 8760 = 4.38 \cdot 10^{-3}.$$

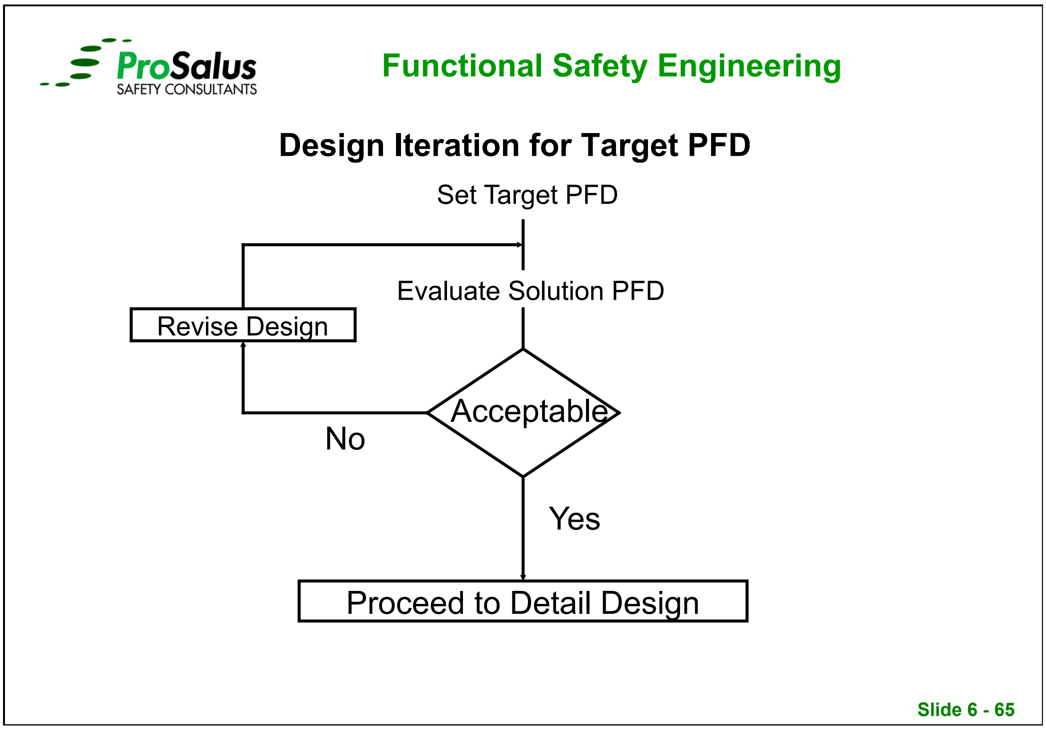
Slide 6 - 63

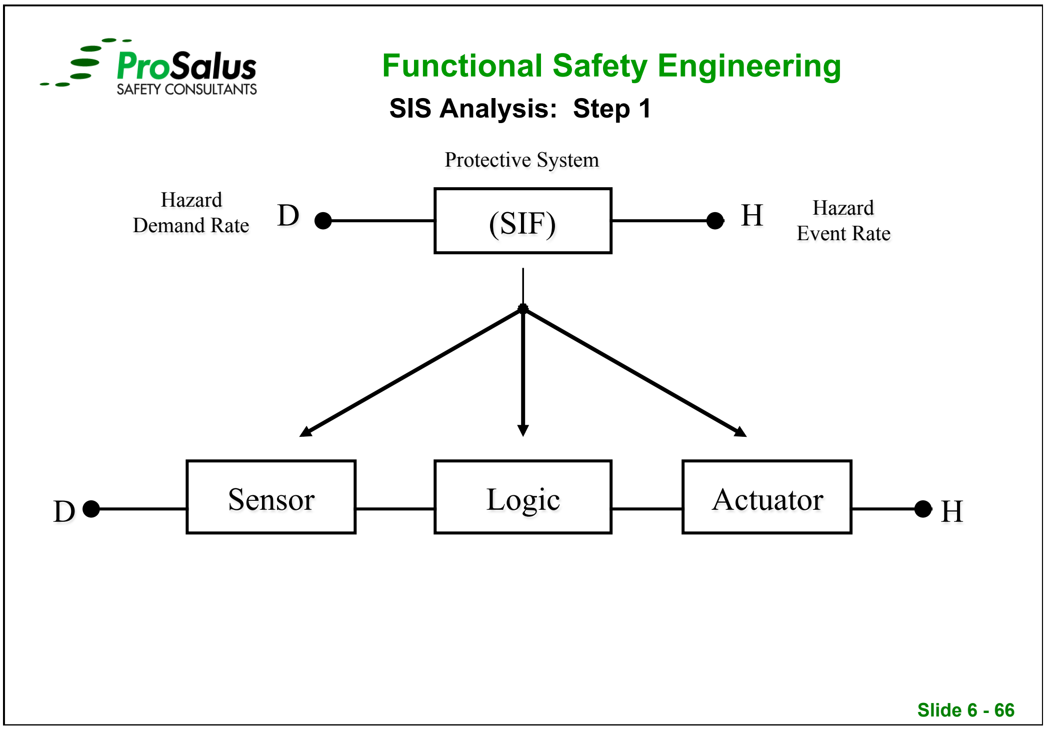
ProSalus SAFETY CONSULTANTS

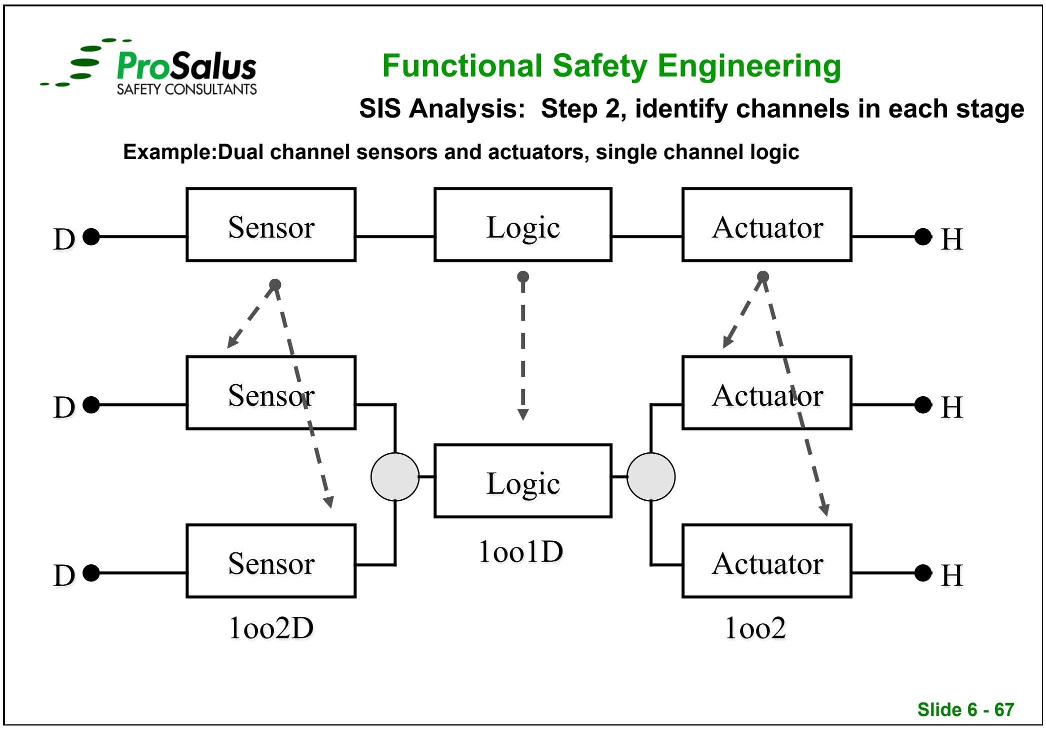
Functional Safety Engineering

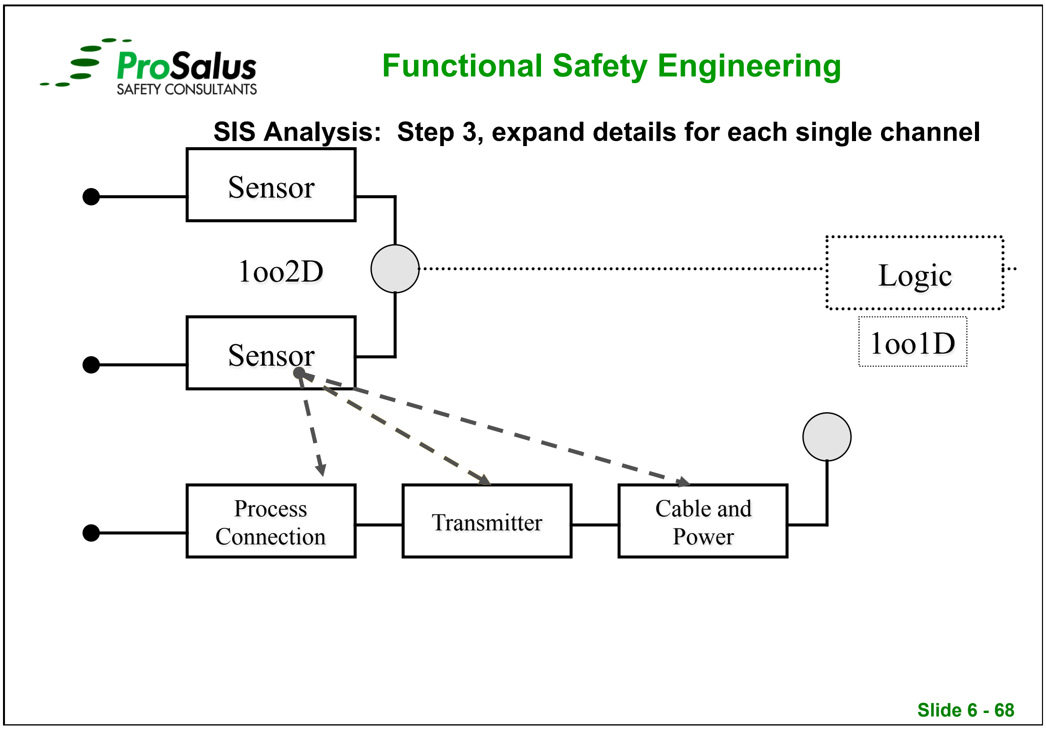
Design Example

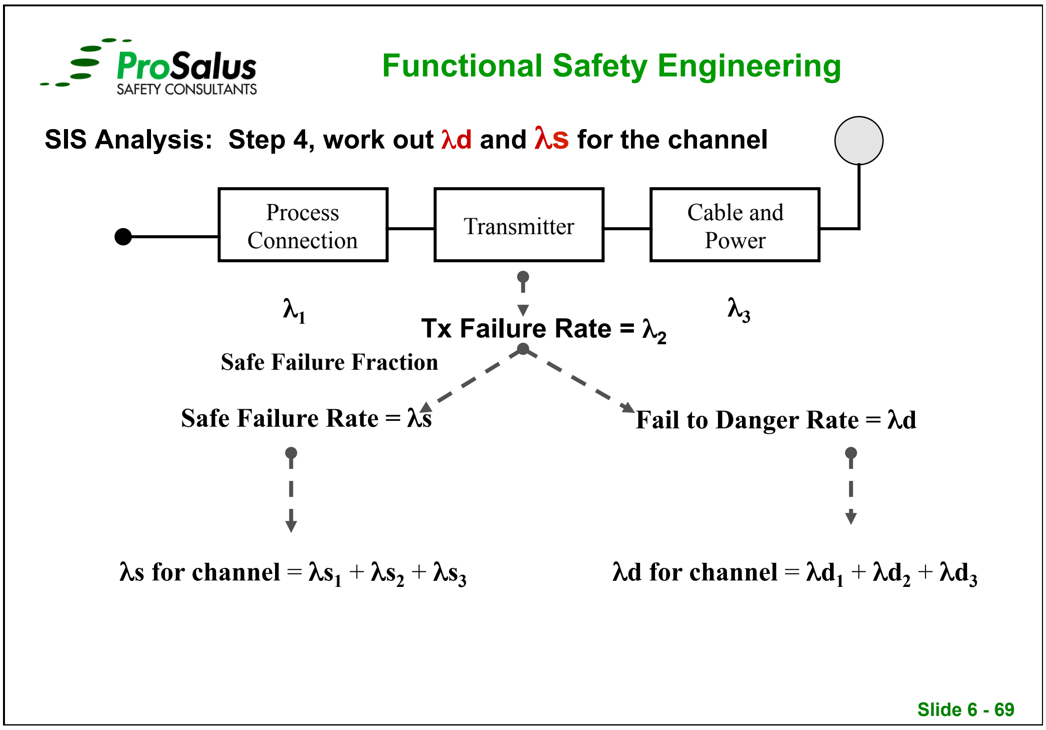
Slide 6 - 64

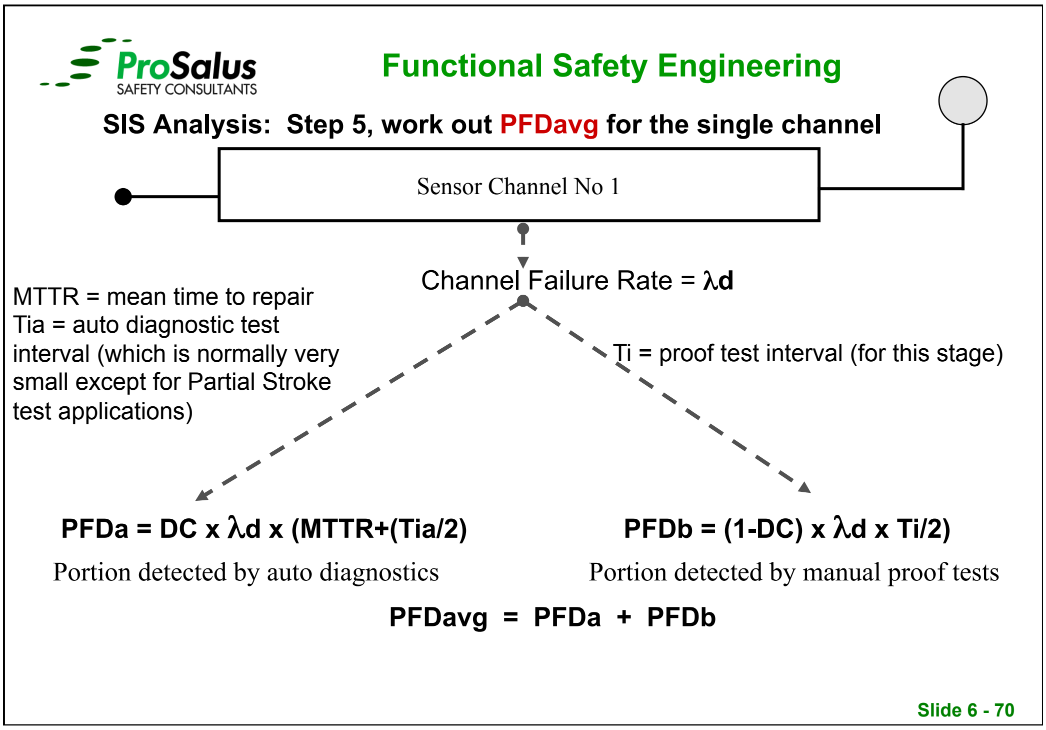

ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
Design Iteration for Target PFD
Set Target PFD
Evaluate Solution PFD
Revise Design
Acceptable
No
Yes
Proceed to Detail Design
Slide 6 - 65


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
SIS Analysis: Step 1
Protective System
Hazard
Demand Rate
D
(SIF)
H
Hazard
Event Rate
D
Sensor
Logic
Actuator
H
Slide 6 - 66


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
SIS Analysis: Step 2, identify channels in each stage
Example:Dual channel sensors and actuators, single channel logic
D
Sensor
Logic
Actuator
H
D
Sensor
Actuator
H
Logic
1oo1D
D
Sensor
Actuator
H
1oo2D
1oo2
Slide 6 - 67


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
SIS Analysis: Step 3, expand details for each single channel
Sensor
1oo2D
Logic
1oo1D
Sensor
Process Connection
Transmitter
Cable and Power
Slide 6 - 68

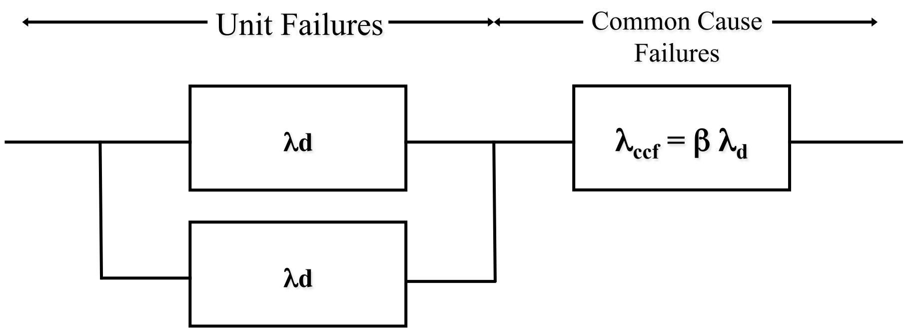

ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
SIS Analysis: Step 4, work out λd and λs for the channel
Process Connection
Transmitter
Cable and Power
λ1
Tx Failure Rate = λ2
λ3
Safe Failure Fraction
Safe Failure Rate = λs
Fail to Danger Rate = λd
λs for channel = λs1 + λs2 + λs3
λd for channel = λd1 + λd2 + λd3
Slide 6 - 69


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
SIS Analysis: Step 5, work out PFDavg for the single channel
Sensor Channel No 1
Channel Failure Rate = λd
MTTR = mean time to repair
Tia = auto diagnostic test interval (which is normally very small except for Partial Stroke test applications)
Ti = proof test interval (for this stage)
PFDa = DC x λd x (MTTR+(Tia/2)
Portion detected by auto diagnostics
PFDb = (1-DC) x λd x Ti/2)
Portion detected by manual proof tests
PFDavg = PFDa + PFDb
Slide 6 - 70

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Beta Factor: Common Cause Failures in redundant SIS channels



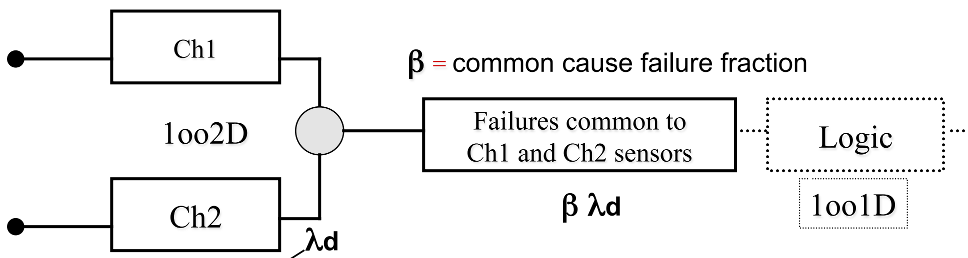
Example: 1002 with common cause failure RBD block

Slide 6 - 71

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 6, find the PFDavg for the 1002D sensor group: Break out the common cause failure fraction for the redundant channels and calculate PFDavgs for each portion



Redundant section:		Common cause section
PFDavg =	+	PFDavg =
$((DC \times \lambda d)^2 \times (MTTR+Tia)^2)$		$((DC \times (\beta \times \lambda d)) \times MTTR)$
$+ (((1-DC \times \lambda d) \times Ti)^2)/3$		$+ ((1-DC \times (\beta \times \lambda d) \times Ti/2)$

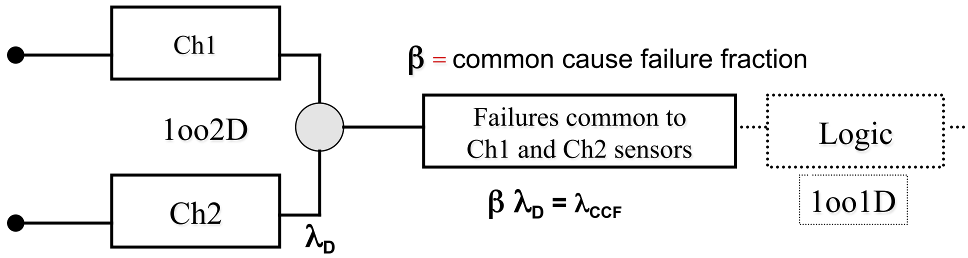
Slide 6 - 72

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example

DC = 70%, λd = 0.01/yr, MTTR = 48 hrs, Tia = 100 msec, Ti = I yr, β = 10%



1002D PFDavg = ((0.7 x 0.01)² x (0.0055)²) + (((1-0.7 x 0.01) x 1)²)/3 = 3.00E-06

+

CCF PFDavg = ((0.7 x (0.1 x 0.01)) x 0.0055) + ((1-0.7 x (0.1 x 0.01) x ½) = 1,54E-04

1002D PFDavg + CCF PFDavg = 3.00E-06 + 1,54E-04 = 1,57E-04

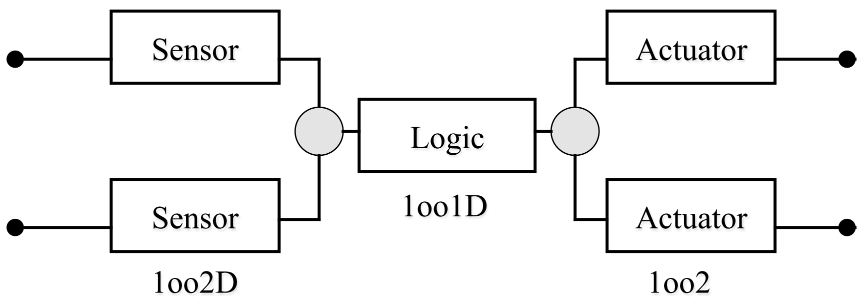
Slide 6 - 73

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SIS Analysis: Step 7, repeat steps 3 to 6 for each stage

Example:Dual channel sensors and actuators, single channel logic



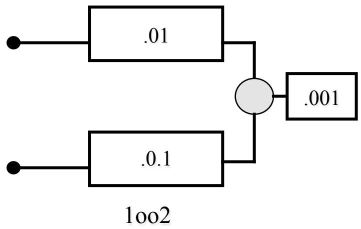
PFDavg for sensors **+** **PFDavg for Logic solver** **+** **PFDavg for actuators**

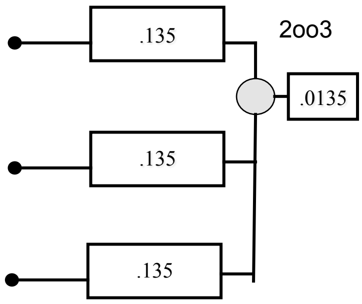
Slide 6 - 74

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example Reducing Spurious Trip Rate





Dual Sensors Spurious
= (2 x 0.01) + (0.1 x 0.01)
= 0.021 trips per yr

2oo3 Sensors Spurious
= 6x λs^2 (MTTR)+ $\beta\ \lambda s$
= (6 x 0.135^2 x 8/8760) +(0.1 x 0.135)
= 0.00001 + 0.0135
= 0. 01351 trips per yr

Slide 6 - 75

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Example evaluation of Diagnostic Coverage for Valve

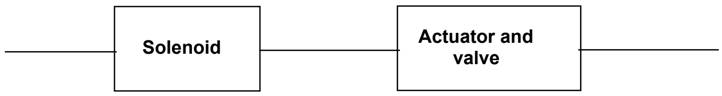
Failure Mode	% Contribution to dangerous failures	%Detection by partial closure test	% Of Dangerous Faults Detected
Actuator spring breakage or jamming	20	70	14
Solenoid fails to vent	5	50	2.5
Positioner fails to trip	5	100	5
Hoses kinked or blocked	10	100	10
Valve stem or rotary shaft stuck	40	70	28
Actuator linkage fault	5	70	3.5
Seating failures of valve causing high leakage. Due to erosion or corrosion	10	0	0
Foreign bodies or sludge preventing full closure	5	0	0
Total	100%		63%

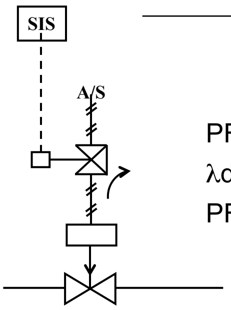
Slide 6 - 76

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Design example: SIL 2 single or double valve decision
Step 1 Single valve with solenoid





Proof test interval Ti = 1 year

PFD1 = λd1 . Ti/2 | PFD2 = λd2 . Ti/2
λd1 = 0.02 /yr | λd2 = 0.04 /yr
PFD1 = 0.01 | PFD2 = 0.02

Overall PFD = 0.03 based on 1 year test interval

Qualifies for SIL 1 only

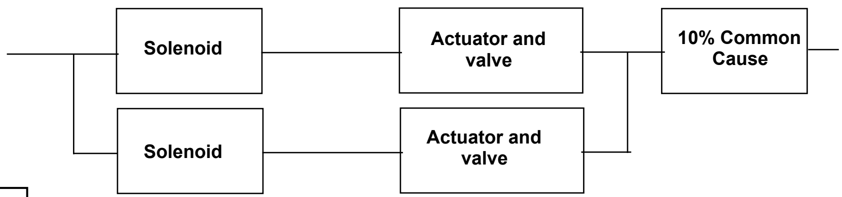
Reliability diagram for single tripping valve

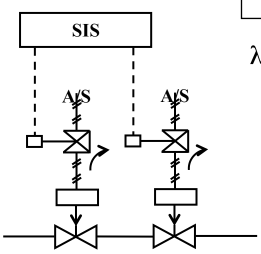
Slide 6 - 77

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Step 2 : Reliability diagram for 1oo2 tripping valves





λd1 = 0.02/yr   λd2 = 0.04/yr

Proof test interval Ti = 1 year

PFD = (λd1+ λd2)² . Ti²/3 + 10%. (λd1+ λd2).Ti/2
= (0.06)² x 1/3 + (0.1 x 0.06) x 1/2
= 0.0042

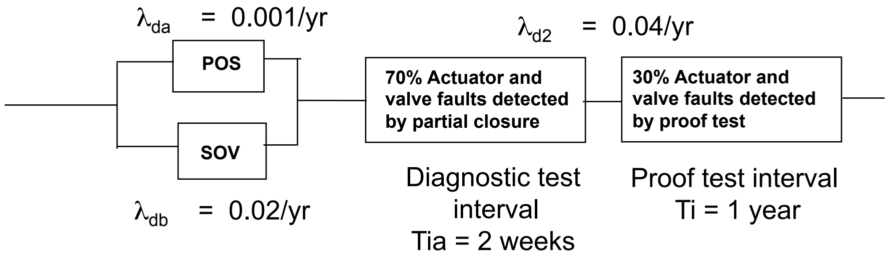
Overall PFD = 4.20E-03 based on 1 year test interval
Qualifies for SIL 2 with adequate margin for sensors and logic

Slide 6 - 78

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Reliability diagram for single tripping valve with Smart Positioner and Partial Closure Testing



$PFD_1 = \lambda_{da} . \lambda_{db} . Ti^2/3$
$PFD_1 = (0.001 \times 0.02) \times 1^2/3$
$PFD_1 = 6.60E\text{-}06$

$PFD_2 = .7\lambda_{d2} . Tia/2$
$PFD_2 = (0.7 \times 0.04) \times 0.038/2$
$PFD_2 = 5.32E\text{-}04$

$PFD_3 = 0.3\lambda_{d2} . Ti/2$
$PFD_3 = (0.3 \times 0.04) \times 1/2$
$PFD_3 = 6.00E\text{-}03$

Overall PFD = 6.54E-03 based on 1 year test interval
Qualifies for SIL 2 with adequate margin for sensors and logic

Slide 6 - 79

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Conclusion for design example

Option 1:

to meet the SIL 2 target: Install 2 block valves and proof test once every 2 years

Option 2:

to meet the SIL 2 target: Install 1 block valve with smart Positioner PS testing every 2 weeks. Proof test once every year.

NB : Both options must satisfy SIL architecture constraints.

Slide 6 - 80

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Commentary on Diagnostic claims for Valves

One attraction of high diagnostic coverage is the improvement in safe failure fraction.

Improved SFF allows reduced Fault Tolerance under IEC 61508. If you can establish high Safe Failure Fraction (SFF) using a smart Positioner you can reduce the number of valves needed to meet a SIL target.

Responsibility remains with end user to justify reduced FT requirements by showing diagnostic coverage and SFF are calculated. Vendors will be keen to assist!

IEC 61508-2 clause 7.4.4.5 should be consulted. See also IEC 61508-6 Annex C

Slide 6 - 81

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Query: Can Diagnostic Coverage of the valve qualify as improved SFF?

Answer: Only if test interval does not add significantly to MTTR and only if safe response or immediate repair is assured. (see 61508-6 annex B).

In practice diagnostic test interval must be at least Ti/10 and should be less than 1 week . (see 61508 annex D table D3). Calculations are required.

If Yes does this mean we can claim > 90% SFF for the valve subsystem?

Answer: Yes

Does this qualify for reduced redundancy?

Answer: Yes it does if PFD figures are satisfied.

Slide 6 - 82

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

SUMMARY

Commonly manufacturers of components and subsystems have no influence on the SIL of the complete safety related system.

SIL-rating of a subsystem makes no sense – in the best case this is an indicator that it would be suitable / has the capability to be part of a *SIL* rated system.

Always the PFDavg or PFH of the safety related system has to be calculated.

Additionally requirements for the avoidance of systematic failures have to be met – 61508 Systematic Capability.

The standard requires an assessment of functional safety capability – Management, Design, Change Control, Implementation, Competency, Operations & Maintainance.

Certificates are not mandatory, and there is no law yet requiring SIL-certificates.

Slide 6 - 83

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Practical Exercise No: 2

SIL Verification Practical

Slide 6 - 84

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Exercise No: 2 – SIL Verification

Task 1 Calculate the single channel PFDavg and spurious trip rate for the high temperature trip example. Draw a single channel reliability block diagram and calculate using the failure rates in the table the PFDavg and the spurious trip rate for each sub system and the overall system using a proof testing interval of 6 months.

Assume the system uses 2 relays, 1 relay in the sensor subsystem and 1 relay in the logic solver subsystem, The trip actuation uses a solenoid valve and to vent the air cylinder on a valve that will drive open and release quench water into the reactor.

Task 2: Redraw the RBD and calculate the PFDavg and spurious trip rate for the SIF using the second diagram showing 3 high temperature transmitters on a reactor configured 2oo3 on the basis of proof testing every 6 months, Beta Factor 10% and MTTR of 24 hours.

The 3 temperature transmitters each transmit to a trip amplifier device that acts as a high temperature trip device leading to a single channel actuation as in task 1

Slide 6 - 85

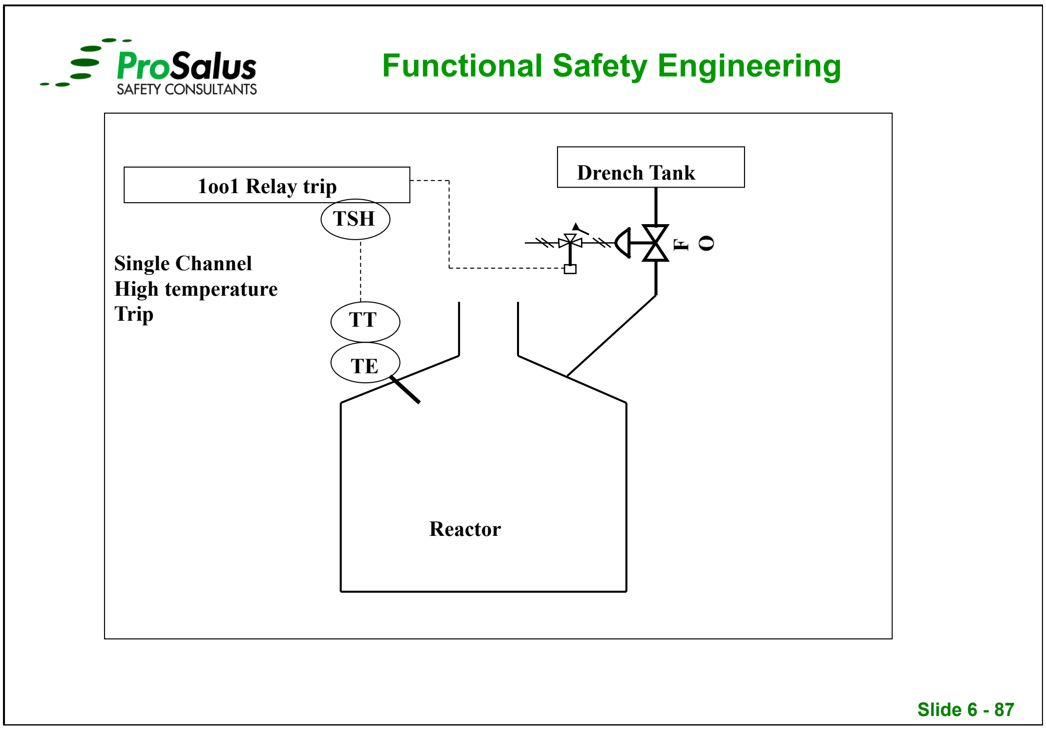
ProSalus SAFETY CONSULTANTS

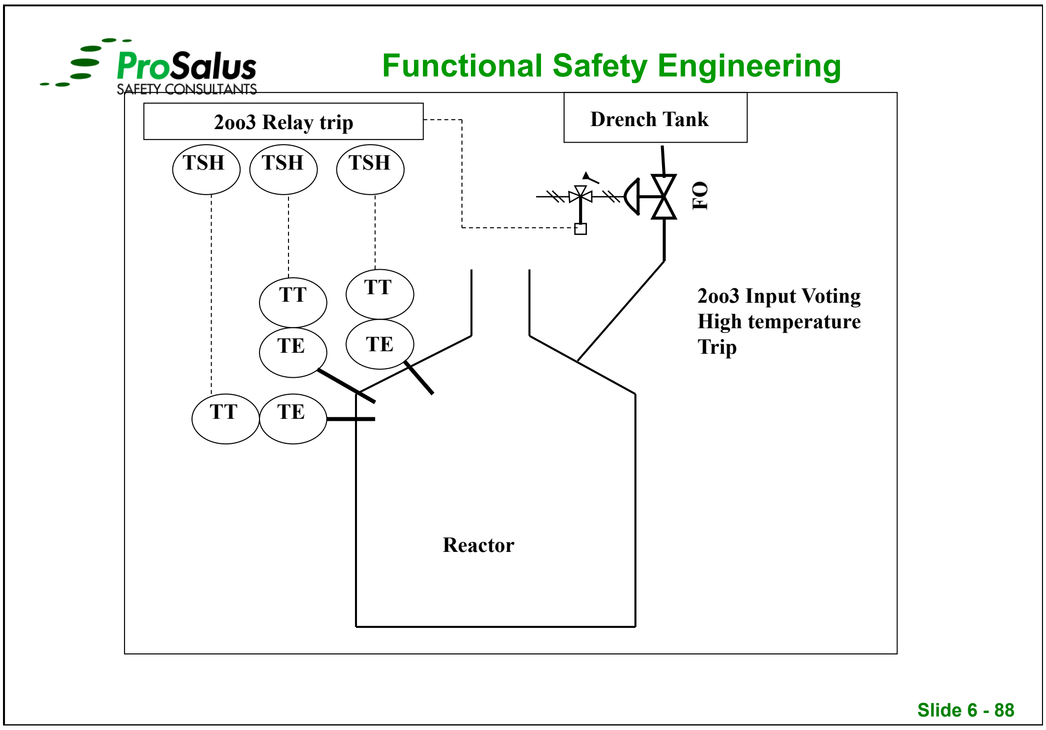
Functional Safety Engineering

Table of fault rates for the Devices

Channel Device	Fail-safe rate per year	Fail –danger rate per year
TE…element	1.5	0.20
TT .Transmitter	0.5	0.05
Cable/terminals	0.01	0.00
TSH….trip amplifier/switch	0.5	0.1
Relay (each)	0.05	0.002
Solenoid Valve	0.04	0.02
Trip Valve	0.4	0.1

Slide 6 - 86


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
1oo1 Relay trip
TSH
Drench Tank
Single Channel
High temperature
Trip
TT
TE
F
O
Reactor
Slide 6 - 87


ProSalus
SAFETY CONSULTANTS
Functional Safety Engineering
2oo3 Relay trip
Drench Tank
TSH
TSH
TSH
FO
TT
TT
TE
TE
2oo3 Input Voting
High temperature
Trip
TT
TE
Reactor
Slide 6 - 88

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Architectures for Low Demand mode of Operation

Based on Reliability Block Diagrams

IEC 61508 2010 Part 6

Slide 6 - 89

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Part 6 Low demand mode – Index of terms

β	The fraction of undetected failures that have a common cause
β_D	The fraction of those failures that are detected by the diagnostic tests, the fraction that have a common cause *($\beta = 2 \times \beta_D$)*
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal 0.5 λ (assumes 50 % dangerous failures and 50 % safe failures)
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)
MTTR	Mean rime to restoration (hour)
PFDG	Average probability of failure on demand for the group of voted channels
T_1	Proof – test interval (h)
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all components in the channel of the subsystem)
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)

Slide 6 - 90

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Part 6 – Low Demand Mode

B.3.2.2.1 1oo1 – System: Single channel where any dangerous failure leads to failure of the safety function when a demand arises.

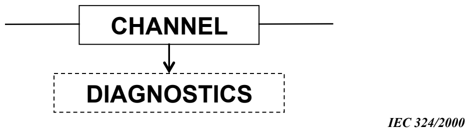


Figure B.4 - 1oo1 Physical Block diagram

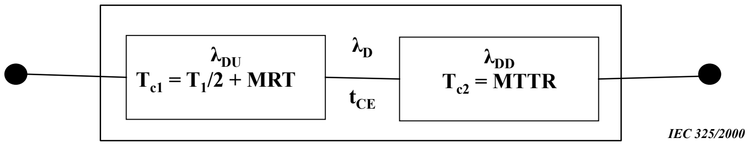


Figure B5 – 1oo1 Reliability Block Diagram

Slide 6 - 91

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo1 – System cont'd

Figure B.5 shows that the channel can be considered to comprise of two components, one with a dangerous failure rate λ_{DU} & the other with a dangerous failure rate λ_{DD}. It is possible to calculate the channel equivalent mean down time t_{CE}, adding the individual down times from both components, t_{c1} and t_{c2}, in direct proportion to each component's contribution to the probability of failure of the channel:

$$t_{CE} = \lambda_{DU} / \lambda_D (T_1 / 2 + MRT) + \lambda_{DD} / \lambda_D \, MTTR$$

For every architecture, the detected dangerous failure rate and the undetected dangerous failure rate are given by

$$\lambda_{DU} = \lambda_D(1\text{-}DC) \; ; \qquad \lambda_{DD} = \lambda_D DC$$

For a channel with down time t_{CE} resulting from dangerous failures

$$PFD = 1 - e^{-\lambda_D t_{CE}}$$
$$\approx \lambda_D t_{CE} \qquad \text{since } \lambda_D t_{CE} << 1$$

Hence, for a 1oo1 architecture, the average probability of failure on demand is

$$PFD_G = (\lambda_{DU} + \lambda_{DD}) t_{CE}$$

Slide 6 - 92

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 Channels

B.3.2.2.2 1oo2 - System

This architecture consists of two channels connected in parallel, such that either channel can process the safety function. Thus there would have to be dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

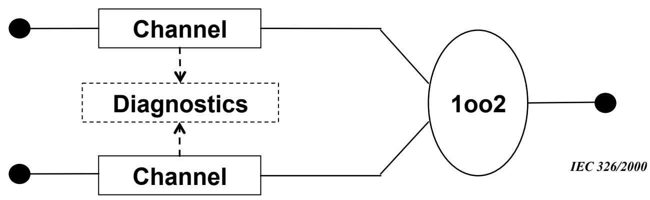


Figure B.6 – 1oo2 physical block diagram

Slide 6 - 93

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2 Channels cont'd

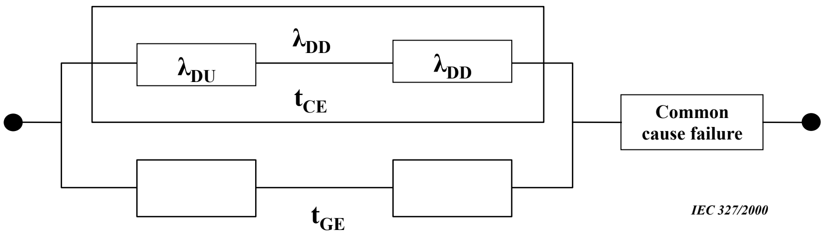


Figure B.7 – 1oo2 reliability block diagram

Figures B.6 and B.7 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1, but now it is necessary to also calculate the system equivalent down time t_{GE}, which is given by

$$t_{GE} = \lambda_{DU} / \lambda_D \, (T_1 / 3 + MRT) + \lambda_{DD} / \lambda_D \, MTTR$$

The average probability of failure on demand for the architecture is

$$PFD_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} \, (T1 / 2 + MRT)$$

Slide 6 - 94

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo2 Channels

B.3.2.2.3 2oo2 – System

This architecture consists of two channels connected in parallel so that both channels need to demand the safety function before it can take place. It is assumed that any diagnostic testing would only report the faults found and would not change any output states or change the output voting.

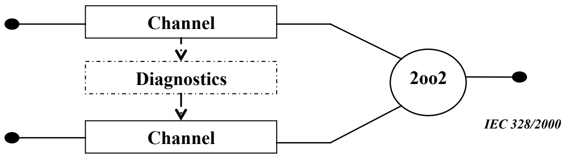


Figure B.8 – 2oo2 physical block diagram

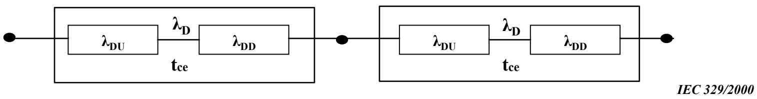


Figure B.9 – 2oo2 reliability block diagram

$$PFD_G = 2\lambda_d t_{ce}$$

Slide 6 - 95

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2D Channels

B.3.2.2.4 1oo2D – System

During normal operation, both channels need to demand the safety function before it can take place. In addiction, if the diagnostic tests in either channel detect a fault then the output voting is adapted so that the overall output state then follows that given by the other channel. If the diagnostic tests find faults in both channels or a discrepancy that cannot be allocated between the channels, either channel can determine the state of the other channel via a means independent of the channel.

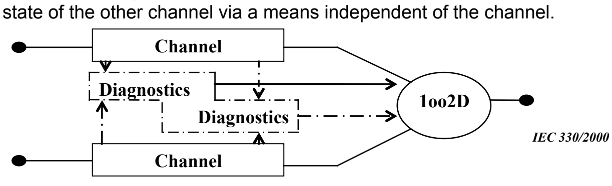


Figure B.10 – 1oo2D physical block diagram

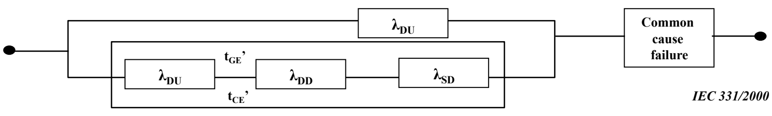


Figure B.11 – 1oo2D reliability block diagram

Slide 6 - 96

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

1oo2D cont'd

The detected Safe failure rate for every channel is given by

$$\lambda_{SD} = \lambda_S DC$$

Figures B.10 and B.11 contain the relevant block diagrams. The values of the equivalent mean down times differ from those given for the other architectures in B.3.2.2 and hence are labelled t_{CE}' and t_{GE}'. Their values are given by:

$$t_{CE}' = (\lambda_{DU} (T_1 / 2 + MRT) + (\lambda_{DD} + \lambda_{SD}) MTTR) / (\lambda_{DU} + (\lambda_{DD} + \lambda_{SD}))$$

$$t_{GE}' = T_1 / 3 + MRT$$

The average probability of failure on demand for the architecture is:

$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})\, t_{CE}'\, t_{GE}' + 2(1\text{-}K)\, \lambda_{DD} t_{CE}' + \beta\lambda_{DU} (T1/2 + MRT)$$

Slide 6 - 97

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo3 Channels

B.3.2.2.5 2oo3 – System

Three channels in parallel with majority voting such that the output state does not change if only one channel changes. It is assumed that any diagnostic testing would report faults only and not change the output state.

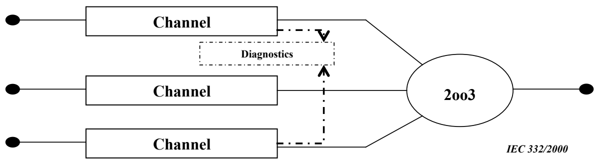


Figure B.12 – 2oo3 physical block diagram

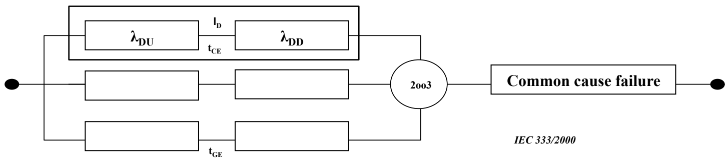


Figure B.13– 2oo3 reliability block diagram

Slide 6 - 98

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

2oo3 cont'd

Figures B.12 and B.13 contain the relevant block diagrams. The value of t_{CE} is as given in B.3.2.2.1 and the value of t_{GE} is as given in B.3.2.2.2 , The average probability of failure on demand for the architecture is:

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} (T1/2 + MRT)$$

B.3.2.2.6 1oo3 – System

Three channels in parallel with a voting arrangement such that the output state follows 1oo3 voting. It is assumed that any diagnostic testing would report faults only and not change the output state. The RBD is as the 2oo3 case but with 1oo3 voting with the value of t_{CE} is as given in B.3.2.2.1 and the value of t_{GE} is as given in B.3.2.2.2 The average probability of failure on demand for the architecture is:

$$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} (T1/2 + MRT)$$

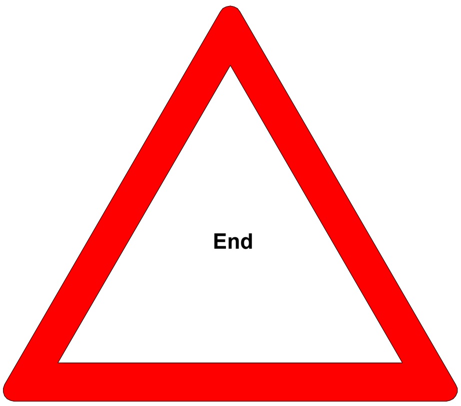
Where

$$t_{G2E} = \lambda_{DU} / \lambda_D (T_1 / 4 + MRT) + \lambda_{DD} / \lambda_D MTTR$$

Slide 6 - 99

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering



Slide 6 - 100

